to which they are affixed becomes unwieldy and easily subject to damage. A special bracket may be required in order to maintain the safety spacing between wires installed on poles to comply with electrical codes or agreements with pole owners. When these traps are damaged, signal leakage and ingress occur. When traps are used in cable systems with underground wiring or in multi-dwelling units, the traps must be installed in pedestals and lock boxes. There is very limited space in these housings.

The flexibility required by some of the provisions of the Cable Act and recent innovations in marketing cannot be realized exclusively with traps. Traps are generally not addressable and do not allow for pay-per-view services. As discussed in Section III of these comments, traps are not flexible enough to allow a cost-effective implementation of the must-carry/retransmission consent and anti buy-through requirements of the 1992 Cable Act. Furthermore, an important recent trend in premium programming is

channels involved and numerous traps will, as noted above, present mechanical and electronic impediments to implementing these new services.

Traps are also not compatible with digital video compression ("DVC") because compressed digital signals convey multiple (perhaps as many as twenty) video programs in a single 6 MHz analog channel space, with the digital information of each compressed channel dispersed throughout the entire 6 MHz space. The trapping of the 6 MHz band, or any portion of it, removes access to all the digital signals in that band. It is not possible to trap out just one or just a few of the compressed signals within that 6 MHz band.

2. Interdiction. Interdiction is a much more expensive example of denial security. Security is accomplished with a jamming device which impairs the signal just before it enters the home. Signals which are desired, pass through to the home without interference. As noted previously, one of the main drawbacks with denial security approaches generally is that the cost of providing the security is born by those people who do not take the service, instead of those customers that generate the revenue from the secured service.

The principal attraction of interdiction is its potential to be compatible with consumer electronics equipment. Since all channels which a subscriber purchases enter the home in a viewable state, no converter or descrambler is needed to view the channels as long as the tuner in the subscriber's VCR and/or TV

is capable of tuning to the cable channels. Thus, the subscriber retains the ability to simultaneously view and record different programs, to consecutively record programs on different channels and to utilize the PIP features which come with his or her consumer electronics equipment. However, in cases where the

fail, the subscriber usually gets all services for free. This situation is difficult to detect since it rarely results in subscriber complaints.

Interdiction also has the disadvantage of being a channel incremental type of security. If more channels are to be protected, more electronics are required. This raises costs and complexity and reduces reliability for several reasons. First, if the housing is full or the maximum capability of the power supply in the housing is reached, such expansion is all but impossible without an expensive rebuild. Second, jamming oscillators are time shared among a number of channels. The amount of sharing a channel receives determines the amount of hiding of the video. Television receivers vary in their ability to produce usable pictures under jamming. Material which may be considered objectionable by some must be more severely jammed. Highly valuable material must likewise be strongly jammed. Jamming adds significant energy to the signal which is fed to the TV or VCR tuner. If a large number of channels are to be controlled, many tuners will not be able to tolerate this additional energy. Distortion in the form of moving bars and background patterns will occur on desired channels. It may then be necessary to add a set-top converter with a superior tuner to allow acceptable pictures. This would defeat the compatibility advantage of interdiction. Third, it is also important that the jamming signals be completely contained within the cable drop. If the jamming signals seep back into the cable system, the

accumulated distortion could reduce the video quality to other subscribers. Fourth, one of the most important trends of the last few years has been the addition of fiber to the cable plant and the removal of electronics. This has increased reliability

and VCRs. Similarly, the provision of OSDs is difficult and clumsy with interdiction outside the home.[18]

Because interdiction hardware is installed in the outside cable plant, its installation costs are very high. The magnitude of the cost is such that it would delay the implementation of fiber optics or video compression for many years because it would consume so much of the available capital for system improvements. Cable must be cut, mechanical support for the devices provided, and significant additional power supplies provided. The installation process is very disruptive to subscribers since cutting the cable interrupts service for all subscribers further down the cable. If interdiction is to be replaced in the future with a more advanced technology, the process of removing the interdiction hardware will be equally expensive and disruptive. Even the important but relatively simple matter of increasing channel capacity is very difficult and expensive. Current interdiction equipment does not extend beyond 550 MHz (approximately 80 video channels).

Finally, three factors have significantly reduced the practicality of interdiction in modern cable systems. First, modern cable systems have expanded their capacity to 75 to 150 analog channels. No interdiction hardware presently is available

---

[18]Indeed, many new ancillary services such as Digital Program Guides, emergency warnings, program advisories and various messaging functions require the use and interaction with OSDs. Such services function best through the use of set top or set back equipment and are difficult to implement where the equipment is located outside the home.

to control such high capacities. Examples of current interdiction hardware in realistic applications show that it can adequately control only 25 or 30 channels. Second, the 1992 Cable Act forces modern cable systems to create tiers of service. This drives up the number of channels which must be addressably controlled beyond the practical limits of most interdiction equipment. Third, interdiction is not compatible with video compression because compressed digital signals place multiple (perhaps as many as twenty) programs in 6 MHz. The jamming of the 6 MHz band, or any portion of it, removes access to all the digital signals in that band. It is not possible to jam out just one or just a few of the compressed signals.

While interdiction technology has been available for a number of years, it has not gained significant market acceptance because of these problems. There are very few suppliers of interdiction hardware and they have very limited product lines. Only Scientific Atlanta is delivering products at this time and only in limited versions suitable for just a few situations.

3. Scrambling. Scrambling is a supply type of security. As such, cost is incurred by the cable operator only in response to a subscription which provides incremental revenue. This localization of expense with subscribers who wish to have a service also minimizes the cost pressures on subscribers who do not want the services which are protected by scrambling. Scrambling is substantially non-channel incremental because additional circuitry is not required in the home if more channels

are offered in the scrambled format. Of course, scramblers at the signal source are required, but their cost is shared by a large number of subscribers. Depending on the method used, scrambling can be very secure and cost effective and yield an excellent picture for the legitimate subscriber while hiding the picture very well from the viewer who does not want it.

Those who wish to receive a scrambled program must have a descrambler which processes the signal so that it can be viewed on an ordinary TV receiver and, unless otherwise processed to prevent it, recorded on an ordinary VCR. Two major types of descramblers have been developed: integrated converter/descramblers and component descramblers. Integrated converter/descramblers contain their own tuner. The cable feed connects directly to the converter/descrambler. The subscriber selects the channel to be viewed on the tuner contained in the converter/descrambler. If it is a scrambled signal, the descrambler processes it to viewable condition. Regardless of the channel selected by the subscriber, the converter/descrambler converts it to a single output channel, usually channel 2 or 3. The tuner in the subscriber's TV or VCR is set permanently to the output channel of the converter/descrambler. Component descramblers, on the other hand, do not contain a tuner. This is analogous to a component audio amplifier as compared to an audio receiver which contains both a tuner and an amplifier. The component descrambler connects directly to the subscriber's TV or VCR through a connector known as the EIA/ANSI 563 Decoder

Interface Connector, to be explained in greater detail in Section IV.C of these comments, infra. The cable drop connects directly to the customer's video equipment. The subscriber can select the desired signal on the tuner contained in the TV or VCR; descrambling can be performed in the internal circuitry of the TV or VCR before the picture is displayed on the screen. Integrated converter/descramblers are by far the most common; component descramblers are very rare today, primarily because few TVs or VCRs are equipped with the EIA/ANSI 563 plug.

A descrambler is able to process only one channel at a time. Therefore, a separate descrambler is required for access to each separate program to be utilized simultaneously. If one scrambled channel is to be watched while another scrambled channel is to be recorded, two descramblers are required. If multiple scrambled programs are to be viewed simultaneously, multiple descramblers are required.

If a system utilizing scrambling is non-addressable, then a "programmable" descrambler could be connected to the subscriber's [redacted]

nominal cost, e.g., by changing an entry code on a computer terminal which sends a message to the affected descrambler to either scramble or descramble the desired channels. Programmable boxes are generally considered to be an obsolete technology because they are easily tampered with and the resulting cable theft is difficult to detect in the subscribers home. In addition, programmable boxes are not feasible for pay-per-view programming since each request would entail switching one box for another for a single programming event. Accordingly, most modern cable systems which utilize scrambling deploy addressable descramblers.

In the majority of current cases, scrambling is used in a hybrid configuration with unscrambled channels and trapped channels. In almost all cases, broadcast and Public, Educational and Governmental Access ("PEG") channels are not scrambled. High penetration premium service channels are often trapped instead of scrambled. Pay-per-view and niche premium services are usually scrambled. Very few cable systems scramble most of their channels. However, as the number of channels increases, the hybrid configuration becomes more difficult to apply, scrambling will become more pervasive. As discussed below, implementation of other provisions of the 1992 Cable Act will also exert pressure to increase the use of scrambling.

There are two major categories of scrambling, R.F. (radio frequency) and baseband. R.F. scrambling operates on the signal in its radio frequency form without demodulation. With one major

exception, it is the method which is oldest, simplest, and generally most vulnerable to compromise. RF scrambling methods depend on suppressing the synchronization pulses which TV receivers require in order to place the picture correctly on the screen. With these synchronization signals suppressed, most TV receivers will display a picture which is either displaced from its correct position on the screen, rolling, or torn into diagonal stripes. The last condition is most successful in hiding the video. The scrambler attenuates the synchronization pulses. The descrambler typically attenuates the non-synchronization portions of the signal so that balance is restored. Frequently, the addressability information is partially or wholly encoded as amplitude modulation on the frequency modulated sound carrier. In addition, separate data carriers are used to carry addressability information. Some TV receivers are more successful at synchronizing to a scrambled signal than others. Thus, in some cases, the subscriber's television set acts as a descrambler and defeats the scrambling. The exception to this is the Zenith Phase Modulation ("PM") method which is much more secure but is in lower penetration.

Baseband scrambling operates on the signal before modulation to scramble it and after demodulation to descramble it. The consequence is much greater flexibility and more options in processing the signal. The earliest forms of baseband scrambling suppressed the synchronization pulses and inverted the video, making it look somewhat like a photographic negative. Much of

the time the picture was torn up into diagonal stripes. At those times when it was not torn up, it appeared as a negative. Advanced methods of baseband scrambling have been developed. These include line shuffling where the picture's lines are interchanged, and line rotation where individual lines are split and their left and right parts interchanged. Still more advanced techniques are under consideration as either new methods or as compatible improvements over methods already in use. Few of these advanced forms of scrambling have been deployed as yet.

The driving force behind the expanded use of scrambling is the subscribers' demand for choice. Premium channels which interest less than half the subscribers and/or which command an interest which comes and goes are most effectively protected by addressable scrambling. Niche programs of interest to a very narrow segment of the subscriber base are another example. Perhaps the most important demand for addressable scrambling is impulse pay-per-view. The ability to purchase a movie, concert, or special event cost effectively and conveniently is a very popular service. Two major impediments to the rapid growth of IPPV are diminishing: channel capacity and movie availability. Experience has proven that just a single or just a couple of channels of IPPV have limited appeal. Subscribers demand a maximization of choice. As cable system capacity expands and multichannel IPPV is implemented, subscribers are buying this service in increasing numbers. As movie studios observe a growing demand for their products, they are making movies

available, and in earlier "windows." To make the service easy to understand and use, many cable operators are offering "Home Theater" services which repeat the same movie on a given channel over and over all day. Several channels configured this way appear to the subscriber to be analogous to the neighborhood multiplex movie theater. This in turn makes the service more interesting and understandable to subscribers. The result is a strong growth in demand for IPPV and its principal enabler, addressable scrambling.

A particularly interesting form of IPPV is Near Video On Demand ("NVOD"). In this format, the same movie is stagger-started on multiple channels. The first practical implementation of this was in Time Warner's Quantum service in Queens, New York. Fifty seven channels are used for IPPV. The top five current movies are started every half hour on four channels each. The subscriber is never more than a half hour away from the start of a popular movie. Less popular movies are started every hour or every two hours. Fifteen different movies are available at all times. Use of this service is greatly facilitated by comprehensive On Screen Displays ("OSDs"), and the ability to force-tune the set-top to the desired channel at the appropriate time and in response to the subscriber's selection. After choosing the movie and its appropriate start time, the subscriber can tune to another channel and browse. At the start time of the subscriber's selection, the tuner is force-tuned to the appropriate channel to watch the movie. Improvements are under

development. If an interruption occurs, the subscriber can press a "pause" button on the remote control. The descrambler's microprocessor keeps track of time. When the subscriber resumes viewing, the microprocessor force-tunes the tuner to the appropriate channel to ensure that none of the movie is missed. Functions such as "reverse" and "fast forward" can be implemented in a convenient but approximate form by force-tuning to the appropriate channel of a set of stagger-started channels. These important features are not possible without force-tuning.

In summary, the most common and most successful method of signal protection is scrambling. It is also the most likely to provide cost effective ways of meeting subscriber demand for multichannel pay-per-view. Scrambling combined with addressability has revolutionized cable and made possible the

deployment of this equipment would be forced to shoulder the additional costs. Under any methodology being considered by the Commission, these additional costs, plus the absence of any technology which is presently as flexible as scrambling in allowing compliance with new regulatory requirements, such as must-carry and anti buy-through, or in accommodating the deployment of new services, such as multichannel IPPV and NVOD, indicate the one unintended consequence of placing limitations on the use of scrambling as a signal security method would be to stifle the development of exciting new services and the deployment of innovative technologies on the horizon.

4. Broadband Descrambling. Broadband descrambling is a signal security concept which descrambles all authorized signals before they enter the residence. As such, it would be highly compatible with consumer electronics products. At this time, there are no products available which implement this approach, it is merely a theoretical concept. It is in the laboratory prototype stage with a number of practical issues yet to be resolved. Moving it out of the laboratory and making it into a product requires substantial funds and several years. There are presently a number of serious concerns.

First, of great concern is the fact that broadband descrambling is fully compatible only with older sync suppression scrambling. To make broadband descrambling possible, signals from blocks of channels are "locked up" so that their horizontal and vertical synchronization pulses occur at the same time. This

reduces the level of security since locating the synchronization times for one channel yields the same information for all channels in the block of channels.

Second, broadband descrambling has only some limited compatibility with the decade old video inversion technique. It is not compatible with more modern analog scrambling approaches. Thus, broadband descrambling severely limits the options for processing the signal and therefore the security which can be obtained. Also limited is the degree of hiding of the signal. To partially compensate for this, broadband descrambling adds optional interdiction. This added security does not help when someone breaks into the cable system by unlawfully tapping into the trunk before the broadband descrambler hardware unit.

Third, broadband descrambling is not compatible with video compression because they are completely unrelated processes. No one has proposed a broadband decompression approach. Even if such an approach were invented, it would result in a huge spectrum requirement. For example, in a 150 channel cable system with 75 channels employing DVC of ten movies per 6 MHz, 750 movie channels are available. If they could be broadband decompressed,

to current efforts to remove these reliability impediments.

- Its channel incremental nature requires more hardware as the number of channels increases.

- As channel capacity expands, the implementation of the electronics becomes more difficult (and expensive) at higher frequencies. There is a practical upper frequency limit. If the hardware is at its maximum channel capacity, expansion to accommodate more channels may not be possible.

- The cost and disruption of installing the hardware in the cable plant similar to that discussed regarding interdiction above.

- The difficulty and cost of replacing it with more advanced technology or replacing it entirely is substantial if security is compromised.

- Off premises equipment increases the difficulty of providing On Screen Displays for subscriber messaging, Digital Program Guides and Near Video On Demand.

- The inability to force-tune the TV's and VCR's tuner makes services such as Near Video On Demand impractical.

5. National Scrambling Standard. A national scrambling standard may be proposed as a method of improving compatibility because the descrambler could be built into TVs or VCRs. If a such standard were implemented, the consumer electronics industry would build descramblers into their TVs and VCRs during the manufacturing process. Theoretically, these descramblers would still be controlled by the cable system which would only authorize the descrambling of the services purchased by the subscriber. This concept has many severe problems.

The most severe problem with a national scrambling standard is the lack of alternatives if it is defeated. The experience in

the U.S., the nation which by far enjoys the highest penetration of cable and subscription video, is that every signal protection scheme, over time, suffers an increasing degree of compromise as pirates develop and market illegal devices. According to OCST, in 1991, over 1,300 theft of service cases were prosecuted nationwide on federal, state and local levels. Seventy-five percent of the more than 250,000 devices seized by law enforcement agencies in 1991 were capable of circumventing addressable technology and allow illegal reception of pay-per-view services. OCST estimates that each illegal decoder sold to a consumer costs the cable industry approximately $3,108 over the decoder's useful life.

When the degree of compromise becomes intolerable from a business standpoint, the cable operator replaces the signal protection hardware. The subscribers' investment in their TVs and VCRs is not affected. If a national scrambling standard was imposed and then later compromised, there would be no way to re-implement security without rendering the subscribers' equipment unusable. This would result in subscriber anger over having to accept an external descrambler. Ironically, the focus of this anger is likely to be the cable operator and not the manufacturer who sold the TV or VCR with the now useless equipment.

Diversity in scrambling methods is a security technique in itself. Diversity complicates the task for those who would go into an underground business of supplying devices which defeat the scrambling. Their market is limited and subject to change.

If one of their customers moves, his illegal descrambler may no longer work. If the cable operator changes scrambling methods, existing illegal devices fail. Time Warner currently utilizes Zenith, Scientific Atlanta, Pioneer, Jerrold and Oak equipment in various cable systems which it operates. Each of the manufacturers produces both R.F. and baseband scrambling equipment. Accordingly, at least ten different scrambling approaches might be employed by various cable systems. Even if one of these existing scrambling techniques were utilized as a national standard, a substantial investment in existing equipment would be rendered obsolete. Ultimately, the cost to replace that equipment would have to be born by cable subscribers and would delay the implementation of promising new technologies that also require significant capital expenditures, such as the deployment of fiber and digital video compression.

No signal protection system is "unbeatable." Those who design signal protection methods have limited time, limited personnel, and limited budgets. They make their designs at a point in the evolution of technology based on assumptions of limited access to that technology. Those who would compromise a security system have unlimited time and the ability to do it at their leisure as a hobby. Their numbers far exceed those of the system designers. It is frequently claimed that digital technology will make possible a truly secure scrambling method. While there are more tools available to the designer of scrambling systems, there are also more tools available to the

attacker. The computer "hacker" has available incredibly complex and capable computing power at very low prices. Networking techniques have made it possible for groups of hackers to rapidly share their results and their computing power. New and even more powerful personal computers and networking systems are promised in the near future. Digital techniques are the domain of hackers and in that sense, going digital facilitates their efforts.

The problem of maintaining signal security is greatly exacerbated in cases where cable operators lose control of security hardware, such as in a situation where descrambling equipment may be legally purchased by subscribers either as part of their TVs and VCRs or as stand-alone units.[19] Subscribers are less reluctant to tamper with their own hardware than with equipment which belongs to the cable company. Prosecution for tampering becomes impossible if the cable operator does not own the descrambler. Moreover, if descramblers become available

---

[19]Although Section 624A(c)(2)(C) requires the Commission to promulgate rules which "promote the commercial availability . . . of converter boxes . . . ," nothing in the statute requires descrambler units to be commercially available. This distinction is crucial. A converter is simply an extended tuner, i.e., a device which allows a TV or VCR to tune to frequencies beyond the range of the tuner contained in the TV or VCR. A descrambler, on the other hand, is a device which is designed to restore an encrypted signal to a viewable state regardless of the frequency on which the signal is carried. As explained in these comments, control by cable operators over deployment of descrambler units is critical to signal security. The Commission should be aware that many local franchises contain provisions which prohibit cable operators from selling or repairing television sets. To the extent that such provisions can be read to prohibit the sale of converters, the Commission should make clear that such provisions are preempted by the 1992 Cable Act.

commercially, it will be extremely difficult to determine whether a particular descrambler was legally manufactured and subsequently tampered with or whether it was originally manufactured to defeat an existing security system. Thus, it would become much more difficult to successfully prosecute the manufacturers of illegal descramblers who, up to now, have been a primary target of theft of service investigation and enforcement.

Allowing subscribers to purchase their own descramblers from a variety of commercially available sources would also take away one of the significant weapons used by cable operators and equipment manufacturers to combat signal theft. In cases where security has been compromised, it is often possible for the manufacturer and cable operator to make a few changes in the security system that will deauthorize the illegal descramblers while allowing authorized subscribers to continue to receive the programming they purchased without the necessity of changing their equipment. This "magic bullet" approach was recently used successfully by Time Warner in its Queens, New York system.[20] Under an amnesty program, a number of customers turned in their illegal descramblers and were converted to legitimate subscribers of the pirated services. This was accomplished without the need to engage in a wholesale replacement of equipment. Such an approach would be difficult or impossible in a situation where descramblers in the field came from a variety of manufacturers.

---

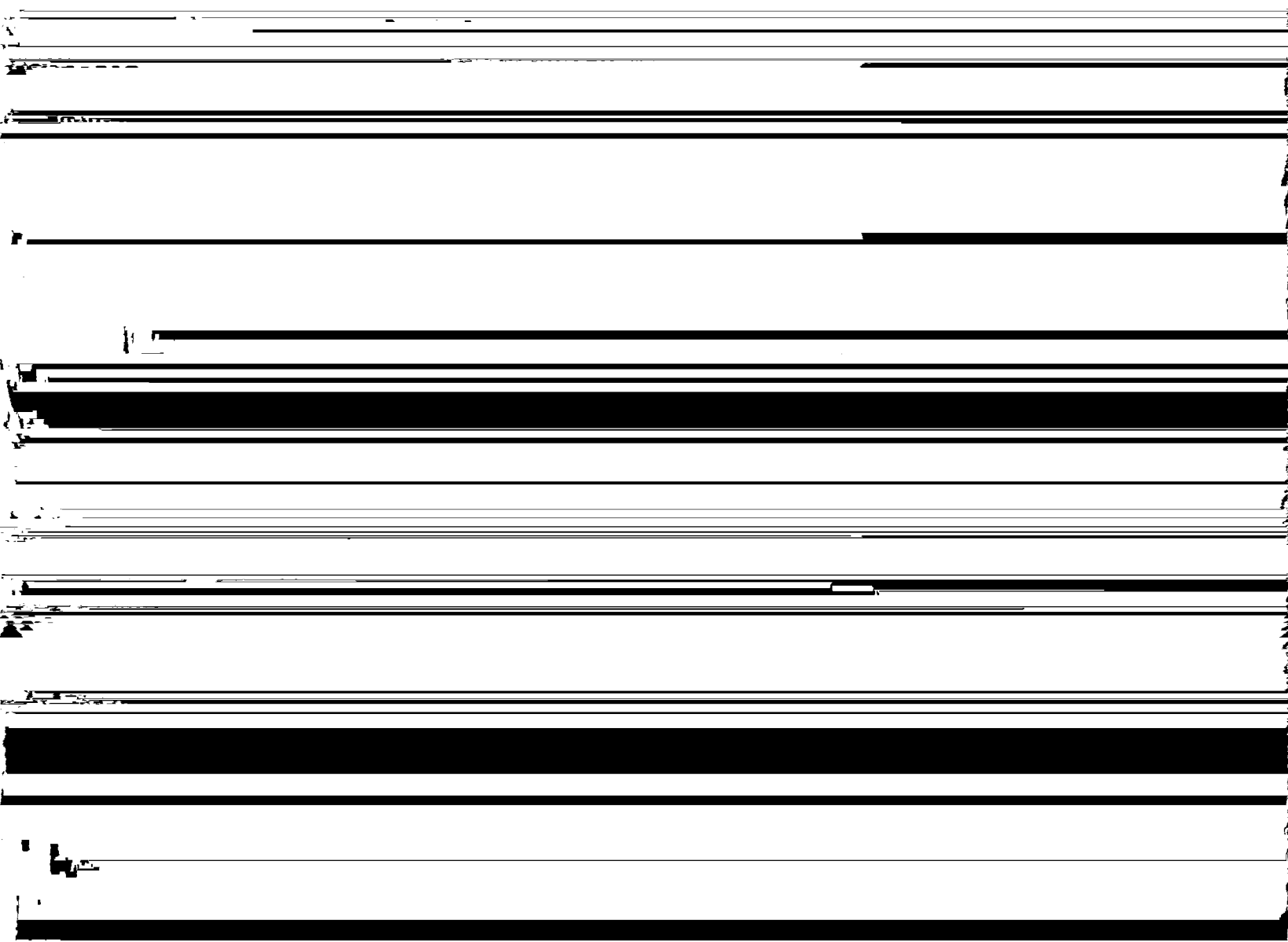
[20]See news articles detailing the incident contained in Appendix 3.

Because of the different manufacturing techniques and processes, it may not be possible to guarantee that the magic bullet would deauthorize only illegal decoders. This would create anger and frustration in cases where legitimate subscribers would no longer be able to use their purchased descrambler on the system.

The consumer electronics industry has resisted techniques which raise their costs because of the difficulty they experience in raising retail prices. The inclusion of descrambling circuitry in the TV or VCR would add substantial costs. The pressure to reduce these costs over time would raise the continuing hazard that cost reduction methods would result in design flaws which could eventually compromise the system and reduce security. There is also the possibility that an unscrupulous off-brand manufacturer with very low market penetration might intentionally consider selling a descrambler implementation which, although functional, was vulnerable to defeat. Once the vulnerability became known, this could result in a significant increase in his sales.

The ultimate defense against compromise of a security system is to replace the compromised scrambling technique with a better one which builds on the lessons learned from a previous defeat. Replacement would create major problems if the subscriber owns the descrambler. It would be tremendously unfair to the majority of subscribers if the hardware they were encouraged to purchase had to be invalidated because a sufficient minority of subscribers acquired illegal descramblers which compromised the

security system. Furthermore, the addition of external descramblers would then likely interfere with features legitimate subscribers had grown accustom to enjoying and which they felt would be continuously useful since they owned the internal descrambler circuits. The duplication of signal processing would reduce signal quality. How would these subscribers be compensated for this loss? Are those who would sell these devices to consumers built into TVs and VCRs going to indemnify both the consumers and the cable operators for the costs of recovering from a breach of security?



dramatically reduce the cost of the network and improve its efficiency. This means that the need for switches and other equipment is not as great in a broadband network and the deployment of such switching equipment will not be as ubiquitous. Accordingly, scrambling and encryption become even more important to secure signals from unauthorized reception as many homes will share access to the same physical network.

One example of the many approaches under consideration will help illustrate this. In narrowband systems, it is necessary to bring a physically separate link to each residence since the capacity of the medium is very limited. The physical separation of the "twisted pair" along with a multiplicity of switches ensures signal security. In a broadband system, many subscribers share access to the same physical network. In a broadband system, fiber links go from the headend to nodes in the neighborhoods. Each node serves around 500 homes. Coaxial cable runs from the node, throughout the neighborhood. Outside the home, the coaxial cable is tapped and a drop connects the network to the home.

Signals are routed to individual homes as follows. Each home is assigned a frequency slot and a compressed NTSC portion of that frequency slot. All switching is accomplished at the cable headend. At the headend, the switch connects the ordered signal source to the appropriate digital multiplexer which assembles a 6 MHz compressed digital signal. That signal is routed the correct modulator which is connected to the specific